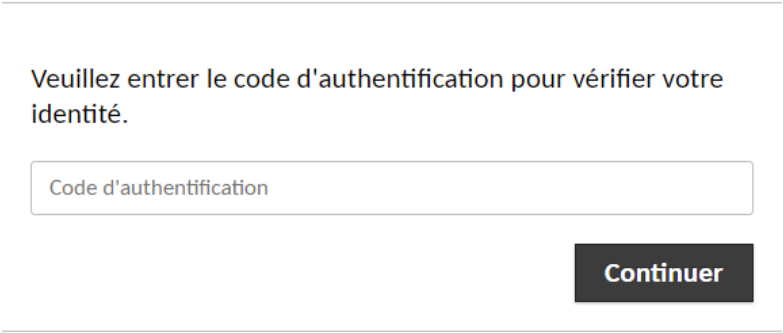
Compte-rendu lundi 26 juin 2023

J'ai effectué deux tâches importantes pour renforcer la sécurité et la surveillance de notre environnement Guacamole Apache.

Tout d'abord, j'ai mis en place la double authentification avec l'extension Time-based One-Time Password (TOTP) sur Guacamole Apache. Cela signifie que lorsqu'un utilisateur entre ses identifiants pour se connecter, il est également demandé de fournir un code à 6 chiffres généré par l'application AuthPoint de WatchGuard. Cette mesure de sécurité supplémentaire permet de protéger nos accès à distance contre les attaques par force brute et les tentatives d'intrusion non autorisées.

Ensuite, j'ai configuré Guacamole Apache pour enregistrer des sessions vidéo de chaque utilisation sur un hôte spécifié. Cela signifie que toutes les activités effectuées sur Guacamole, y compris les actions de l'utilisateur, les commandes exécutées et les écrans affichés, seront enregistrées sous forme de vidéos. Ce type de surveillance nous offre une traçabilité complète des sessions, ce qui est utile pour l'audit, la résolution des problèmes et la sécurité globale de notre système.



Grâce à ces deux mesures mises en place, nous avons considérablement renforcé la sécurité de notre environnement Guacamole Apache. La double authentification garantit que seules les personnes disposant des identifiants corrects et du code TOTP peuvent se connecter, réduisant ainsi les risques d'accès non autorisés. De plus, les enregistrements vidéo de chaque session permettent une surveillance complète et une analyse approfondie des activités effectuées, ce qui peut être essentiel pour détecter et prévenir toute utilisation abusive ou suspecte.

Compte-rendu mardi 27 juin 2023

Je viens de paramétrer le multipathing sur notre système. J'ai effectué les modifications nécessaires dans le fichier de configuration `**/etc/multipath.conf**` pour répondre à nos besoins. Voici ce que j'ai fait :

Tout d'abord, j'ai configuré les paramètres par défaut en activant les options sur « yes » **`user_friendly_names`, `find_multipaths` et `no_path_retry`**. Cela améliorera la convivialité, la détection des multipathes et la gestion des échecs de chemin.

Ensuite, j'ai ajouté des règles dans la section **`blacklist`** pour exclure certains types de périphériques tels que les lecteurs de disquette et les disques durs IDE. J'ai également exclu les périphériques VMware de la gestion du multipathing en spécifiant le vendeur et le produit dans la liste noire.

Enfin, j'ai configuré un bloc `device` spécifique pour les périphériques VMware de type "Virtual disk". J'ai défini la politique de regroupement des chemins, le sélecteur de chemin, le vérificateur de chemin, le basculement et le poids des chemins selon nos besoins.

Une fois les modifications terminées, j'ai redémarré le service `multipathd` en utilisant la commande `sudo systemctl restart multipathd`. Le service a redémarré avec succès, sans aucune erreur.

Ce paramétrage du multipathing permettra d'améliorer la résilience et les performances de notre stockage en utilisant plusieurs chemins vers les périphériques de stockage. Cela permettra de répartir la charge et de fournir une redondance en cas de défaillance d'un chemin.

J'ai vu ceci car je me suis aperçu qu'en regardant les logs avec tail -f /var/log/syslog, je voyais ceci :

```
root@vm-guaca-cm:~# tail -f /var/log/syslog
Jun 30 13:22:26 vm-guaca-cm multipathd[42361]: sda: failed to get sysfs uid: Invalid argument
Jun 30 13:22:26 vm-guaca-cm multipathd[42361]: sda: failed to get sgio uid: No such file or directory
Jun 30 13:22:31 vm-guaca-cm multipathd[42361]: sda: add missing path
Jun 30 13:22:31 vm-guaca-cm multipathd[42361]: sda: failed to get udev uid: Invalid argument
Jun 30 13:22:31 vm-guaca-cm multipathd[42361]: sda: failed to get sysfs uid: Invalid argument
Jun 30 13:22:31 vm-guaca-cm multipathd[42361]: sda: failed to get sgio uid: No such file or directory
Jun 30 13:22:36 vm-guaca-cm multipathd[42361]: sda: add missing path
Jun 30 13:22:36 vm-guaca-cm multipathd[42361]: sda: failed to get udev uid: Invalid argument
Jun 30 13:22:36 vm-guaca-cm multipathd[42361]: sda: failed to get sysfs uid: Invalid argument
```

Le fichier multipath.conf ressemble à ceci : et il n'y a plus d'erreur lorsque l'on regarde les logs.

```
defaults {
   user_friendly_names yes
}

blacklist {
   devnode "^sd[a-z]"
}

devices {
   device {
      vendor "VMware"
      product "Virtual_disk"
      path_grouping_policy "failover"
      path_selector "round-robin 0"
      features "1 queue_if_no_path"
      hardware_handler "1 alua"
      prio "alua"
      failback "immediate"
   }
}
```

Compte-rendu mercredi 28 juin 2023

Aujourd'hui, j'ai entrepris la mise en place de l'extension LDAP dans Guacamole. L'objectif était d'utiliser l'authentification LDAP pour permettre aux utilisateurs de se connecter à Guacamole en utilisant leurs identifiants Active Directory (AD). Voici un récapitulatif des points clés de cette démarche :

1. Objectif :

L'extension LDAP dans Guacamole permet d'intégrer l'authentification à un annuaire LDAP, tel qu'Active Directory, pour simplifier la gestion des utilisateurs et des accès aux serveurs distants. En utilisant l'authentification LDAP, les utilisateurs peuvent se connecter à Guacamole en utilisant leurs identifiants AD, évitant ainsi la nécessité de créer et de gérer des comptes d'utilisateurs distincts dans Guacamole.

2. Problèmes rencontrés :

Lors de la configuration initiale, j'ai rencontré plusieurs problèmes. Tout d'abord, j'ai constaté que les utilisateurs AD n'étaient pas automatiquement créés dans la base de données Guacamole malgré l'ajout de la configuration `**ldap-add-new-users: true**`. De plus, les tentatives de recherche d'utilisateurs dans l'annuaire LDAP ont échoué, générant des erreurs de connexion ou des erreurs indiquant l'absence d'objets ou de contextes dans l'annuaire LDAP.

3. Actions entreprises :

Pour résoudre ces problèmes, j'ai vérifié attentivement la configuration LDAP dans le fichier `**guacamole.properties**`. J'ai confirmé que les informations de connexion, telles que l'adresse IP ou le nom d'hôte du serveur LDAP, le port LDAP, le DN de la base d'utilisateurs, ainsi que les identifiants de l'utilisateur de recherche LDAP, étaient correctes. De plus, vous avez vérifié les permissions accordées à l'utilisateur LDAP pour s'assurer qu'il avait les droits nécessaires pour rechercher les utilisateurs dans l'annuaire AD.

4. Résultats :

Malgré mes vérifications, les problèmes persistaient. Les comptes utilisateurs AD n'étaient pas créés automatiquement dans la base de données Guacamole, et les tentatives de recherche d'utilisateurs dans l'annuaire LDAP échouaient. Vous avez consulté les journaux d'erreurs de Guacamole pour obtenir des informations supplémentaires, mais aucune erreur spécifique n'a été identifiée.

Compte-rendu jeudi 29 juin 2023

Depuis ma dernière mise à jour, j'ai réussi à me connecter avec les utilisateurs de mon Active Directory (AD). J'ai effectué des modifications dans le fichier `**guacamole.properties**`, qui ressemble maintenant à ceci, grâce à l'aide du site officiel de Guacamole*:

```
# Activation de l'authentification LDAP
ldap-auth: true

# Adresse IP ou nom d'hôte du serveur LDAP (contrôleur de domaine)
ldap-hostname: 192.168.200.81

# Port LDAP (par défaut: 389)
ldap-port: 389

# Nom de la base DN (Distinguished Name) pour les utilisateurs
ldap-user-base-dn: ou=Spgd,dc=springfield,dc=local

# Nom de l'attribut LDAP
ldap-username-attribute: sAMAccountName

# Nom d'utilisateur et mot de passe pour la recherche dans l'annuaire
ldap-search-bind-dn: cn=ldap lr. readonly,ou=Spgd,dc=springfield,dc=local
ldap-search-bind-password: Issurtille1+

# Propriété facultative - si votre annuaire AD utilise un protocole SSL/TLS
ldap-encryption-method: none

# Ajoute les comptes d'utilisateurs AD dans la base de données Guacamole
ldap-add-new-users: true
```

Actuellement, je peux me connecter avec les utilisateurs de mon Active Directory, ce qui est une avancée positive. Cependant, je rencontre toujours un problème avec la création automatique des comptes utilisateurs dans la base de données Guacamole. En conséquence, lorsque les utilisateurs se connectent, aucune connexion à des machines virtuelles n'est disponible. De plus, lorsque je me connecte en tant qu'administrateur sur Guacamole, je ne vois pas les comptes utilisateurs provenant de l'Active Directory.

Voici ce qu'on peut voir lorsque qu'on regarde les logs avec tail -f /var/log/tomcat9/catalina.out

```
[2023-06-30 12:36:02] [info] 12:36:02.666 [http-nio-8080-exec-6] INFO  o.a.g.a.l.AuthenticationProviderService - User "l.simpson" was successfully authenticated by LDAP server "192.168.200.81".
[2023-06-30 12:36:02] [info] 12:36:02.666 [http-nio-8080-exec-6] INFO  o.a.g.r.auth.AuthenticationService - User "l.simpson" successfully authenticated from 10.2.43.48.
[2023-06-30 12:36:02] [info] 12:36:02.678 [http-nio-8080-exec-6] INFO  o.a.g.auth.jdbc.user.UserService - Data cannot be stored for user "l.simpson" as they do not have an account within the database. If this is unexpected, consider allowing automatic creation of user accounts.
[2023-06-30 12:36:09] [info] 12:36:09.563 [http-nio-8080-exec-6] INFO  o.a.g.a.l.AuthenticationProviderService - User "b.simpson" was successfully authenticated by LDAP server "192.168.200.81".
[2023-06-30 12:36:09] [info] 12:36:09.563 [http-nio-8080-exec-6] INFO  o.a.g.r.auth.AuthenticationService - User "b.simpson" successfully authenticated from 10.2.43.48.
[2023-06-30 12:36:09] [info] 12:36:09.573 [http-nio-8080-exec-6] INFO  o.a.g.auth.jdbc.user.UserService - Data cannot be stored for user "b.simpson" as they do not have an account within the database. If this is unexpected, consider allowing automatic creation of user accounts.
```

Je suis conscient que cette fonctionnalité de création automatique des comptes utilisateurs est essentielle pour permettre aux utilisateurs de Guacamole d'accéder aux machines virtuelles. Je vais continuer à investiguer cette problématique et chercher des solutions appropriées. Il est possible que des ajustements supplémentaires soient nécessaires dans la configuration de Guacamole ou dans la gestion des droits d'accès dans l'Active Directory.

Je reste déterminé à résoudre ces problèmes afin de garantir une expérience fluide pour les utilisateurs de Guacamole et d'exploiter pleinement les avantages de l'intégration avec l'Active Directory. Je continuerai à effectuer des recherches, à consulter des ressources spécialisées et à explorer les options disponibles pour résoudre ces problèmes.

* https://guacamole.apache.org/doc/gug/ldap-auth.html

Compte-rendu vendredi 30 juin 2023

Aujourd'hui, j'ai rédiger comment j'ai installé l'extension **Guacamole History Recording Storage** sur la VM qui héberge Guacamole.apache. J'ai trouvé un tutoriel très utile sur le site https://www.it-connect.fr/tuto-apache-guacamole-bastion-rdp-ssh-debian/#B_Creer_un_enregistrement_video_des_sessions qui m'a guidé tout au long du processus d'installation. Voici un résumé des étapes que j'ai suivies :

1. Tout d'abord, j'ai téléchargé le fichier `**guacamole-history-recording-storage-1.5.2.tar.gz**` à partir de la source recommandée.

2. Ensuite, j'ai extrait les fichiers de l'archive téléchargée à l'aide de la commande `**tar -xvf guacamole-history-recording-storage-1.5.2.tar.gz**`.

3. J'ai déplacé '**guacamole-history-recordy-storage-1.5.2**' dans le répertoire d'extensions.

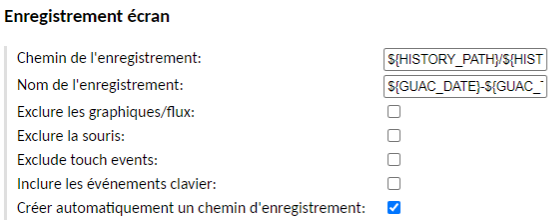
4. J'ai redémarré le service tomcat9 pour prendre en compte les modifications en utilisant la commande appropriée (`**systemctl restart tomcat9**`).

5. J'ai crée le répertoire ou sera enregistré les enregistrements vidéos : **mkdir -p /var/lib/guacamole/recordings** et donné des autorisations : **'chown root:tomcat /var/lib/guacamole/recordings'** et **'chmod 2750 /var/lib/guacamole/recordings'.**

6. Sur chaque configuration des VM que j'ai enregistré dans Guacamole, j'ai ajouté ces deux lignes la dans la parties « Enregistrement video » :

Chemin de l'enregistrement : **${HISTORY_PATH}/${HISTORY_UUID}**
Nom de l'enregistrement : **${GUAC_DATE}-${GUAC_TIME} - RDP - ${GUAC_USERNAME}**

Ce qui donne :



7. Après avoir enregistré les modifications, j'ai redémarré le service Guacamole pour appliquer la configuration.

Maintenant, grâce à l'extension **Guacamole History Recording Storage**, j'ai la possibilité d'enregistrer les sessions de mes utilisateurs pour une utilisation ultérieure. Cela me permet de revoir les sessions passées, d'analyser les activités et d'améliorer la sécurité et la conformité.

Il restera cependant deux problèmes que je rencontre actuellement :

- Le premier est celui ou les utilisateurs utilisant leur identifiants et mots de passe enregistré sur AD, ne sont pas créés automatiquement dans la base de données de Guacamole.

- Le deuxième est celui ou lorsque je me connecte avec mon compte administrateur sur mon compte Guacamole, et que je souhaite prendre à distance une VM, et bien je me fais déconnecter quelques secondes après de la machine virtuelle et cela pour toutes les VM Windows que je prends en RDS depuis Guacamole.

- J'ai vérifié que le pare-feu était activé et ne bloquait pas les connexions RDP, et j'ai regardé si les ports étaient ouverts :

```
root@vm-guaca-cm:~# systemctl status ufw
ufw.service - Uncomplicated firewall
     Loaded: loaded (/lib/systemd/system/ufw.service; enabled; vendor preset: enabled)
     Active: active (exited) since Thu 2023-06-29 13:43:58 UTC; 23h ago
       Docs: man:ufw(8)
   Main PID: 39289 (code=exited, status=0/SUCCESS)
      Tasks: 0 (limit: 9389)
     Memory: 0B
     CGroup: /system.slice/ufw.service
juin 29 13:43:58 vm-guaca-cm systemd[1]: Starting Uncomplicated firewall...
juin 29 13:43:58 vm-guaca-cm systemd[1]: Finished Uncomplicated firewall.
```

```
sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
389                        ALLOW       Anywhere
636                        ALLOW       Anywhere
3389                       ALLOW       Anywhere
22                         ALLOW       Anywhere
8080                       ALLOW       Anywhere
389 (v6)                   ALLOW       Anywhere (v6)
636 (v6)                   ALLOW       Anywhere (v6)
3389 (v6)                  ALLOW       Anywhere (v6)
22 (v6)                    ALLOW       Anywhere (v6)
8080 (v6)                  ALLOW       Anywhere (v6)
```

On peut voir que le protocole RDP (3389) n'est pourtant pas bloqué par le pare-feu, à ce jour je ne sais pas trop pourquoi je n'arrive pas à me connecter à une machine virtuelle en RDP depuis Guacamole, alors que depuis mon ordinateur physique je peux, j'ai pourtant bien vérifié les configurations des machines dans « nouvelle connexion » (identifiant / mots de passe / domaine etc.)

On voit d'ailleurs bien sur la capture d'écran ci-dessous que les ports qui nous intéressent sont sur écoute :

```
root@vm-guaca-cm:~# ss -tuln
Netid              State              Recv-Q             Send-Q                         Local Address:Port                         Peer Address:Port             Process
udp                UNCONN             0                  0                              127.0.0.53%lo:53                                0.0.0.0:*
udp                UNCONN             0                  0                    192.168.200.77%ens160:68                                0.0.0.0:*
tcp                LISTEN             0                  4096                           127.0.0.53%lo:53                                0.0.0.0:*
tcp                LISTEN             0                  5                                    0.0.0.0:4822                              0.0.0.0:*
tcp                LISTEN             0                  128                                  0.0.0.0:22                                0.0.0.0:*
tcp                LISTEN             0                  1024                                 0.0.0.0:389                               0.0.0.0:*
tcp                LISTEN             0                  80                                 127.0.0.1:3306                              0.0.0.0:*
tcp                LISTEN             0                  2                                      [::1]:3350                                 [::]:*
tcp                LISTEN             0                  128                                     [::]:22                                 [::]:*
tcp                LISTEN             0                  2                                          *:3389                                 *:*
tcp                LISTEN             0                  1024                                    [::]:389                                [::]:*
tcp                LISTEN             0                  100                                        *:8080                                 *:*
```

Au moment où j'écris le compte-rendu de ce jour, je me rends compte que ma VM Ubuntu n'est pas à l'heure, donc j'exécute la commande suivante : **sudo timedatectl set-timezone Europe/Paris**

Avec la commande **tail -f /var/log/tomcat9/catalina.out**, on peut voir que la connexion à une VM n'a pas durée très longtemps.

```
[2023-06-30 13:17:14] [info] 13:17:14.669 [http-nio-8080-exec-3] INFO  o.a.g.tunnel.TunnelRequestService - User "techoci" connected to connection "2".
[2023-06-30 13:17:19] [info] 13:17:19.537 [Thread-4] INFO  o.a.g.tunnel.TunnelRequestService - User "techoci" disconnected from connection "2". Duration: 4862 milliseconds
```

De même avec **tail -f /var/log/syslog**

```
Jun 30 13:51:12 vm-guaca-cm guacd[78710]: Connection "$5f6556da-1e1a-4d07-813a-0b82421a44c1" removed.
Jun 30 13:51:15 vm-guaca-cm tomcat9[73205]: 13:51:15.412 [Thread-14] INFO  o.a.g.tunnel.TunnelRequestService - User "techoci" disconnected from connection "2". Duration: 4933 milliseconds
Jun 30 13:54:59 vm-guaca-cm guacd[78710]: Creating new client for protocol "rdp"
Jun 30 13:54:59 vm-guaca-cm guacd[78710]: Connection ID is "$bb8eefd7-a072-4a48-83ac-6722b7df08d4"
Jun 30 13:54:59 vm-guaca-cm guacd[82367]: No security mode specified. Defaulting to security mode negotiation with server.
Jun 30 13:54:59 vm-guaca-cm guacd[82367]: Resize method: none
Jun 30 13:54:59 vm-guaca-cm guacd[82367]: No clipboard line-ending normalization specified. Defaulting to preserving the format of all line endings.
Jun 30 13:54:59 vm-guaca-cm guacd[82367]: User "@956c24dc-56bb-4c4b-882c-67522084fe9d" joined connection "$bb8eefd7-a072-4a48-83ac-6722b7df08d4" (1 users now present)
Jun 30 13:54:59 vm-guaca-cm guacd[82367]: Recording of session will be saved to "/var/lib/guacamole/recordings/7ca0e391-4af9-310e-ae41-f3c7c4f4e36e/20230630-135458 - RDP - techoci".
Jun 30 13:54:59 vm-guaca-cm guacd[82367]: Loading keymap "base"
Jun 30 13:54:59 vm-guaca-cm guacd[82367]: Loading keymap "fr-fr-azerty"
Jun 30 13:54:59 vm-guaca-cm tomcat9[73205]: 13:54:59.035 [http-nio-8080-exec-3] INFO  o.a.g.tunnel.TunnelRequestService - User "techoci" connected to connection "3".
Jun 30 13:55:00 vm-guaca-cm guacd[82367]: Connected to RDPDR 1.13 as client 0x0004
Jun 30 13:55:01 vm-guaca-cm kernel: [107432.872500] guacd[82372]: segfault at 0 ip 00007f3ed7759bc0 sp 00007f3ec5ce08a8 error 6 in libc-2.31.so[7f3ed75f0000+178000]
Jun 30 13:55:01 vm-guaca-cm kernel: [107432.872519] Code: 9d 48 81 fa 80 00 00 00 77 19 c5 fe 7f 07 c5 fe 7f 47 20 c5 fe 7f 44 17 e0 c5 fe 7f 44 17 c0 c5 f8 77 c3 48 8d 8f 80 00 00 00 <c5> fe 7f 07 48 83 e1 80 c5 fe 7f 44 17 e0 c5 fe 7f 47 20 c5 fe 7f
Jun 30 13:55:01 vm-guaca-cm guacd[78710]: Connection "$bb8eefd7-a072-4a48-83ac-6722b7df08d4" removed.
Jun 30 13:55:03 vm-guaca-cm tomcat9[73205]: 13:55:03.974 [Thread-16] INFO  o.a.g.tunnel.TunnelRequestService - User "techoci" disconnected from connection "3". Duration: 4938 milliseconds
```

On voit une erreur de segmentation (segfault) qui est détectée dans le processus guacd, ce qui provoque la suppression de la connexion RDP. Cela peut être dû à un problème avec le guacd lui-même ou à une incompatibilité avec la configuration de votre système.

COMPTE-RENDU en bref de la semaine : (message envoyé sur ECLAT)

Compte-rendu hebdomadaire du 26 au 30 juin 2023 :

Cette semaine, j'ai réalisé plusieurs activités visant à renforcer la sécurité et l'efficacité de notre environnement Guacamole Apache, à améliorer la gestion des chemins multiples (multipathing) et à intégrer l'authentification LDAP.

En début de semaine, j'ai mis en place la double authentification avec l'extension TOTP sur Guacamole Apache. Cela permet de protéger nos accès à distance contre les attaques par force brute et les tentatives d'intrusion non autorisées. De plus, j'ai configuré Guacamole Apache pour enregistrer des sessions vidéo, ce qui offre une traçabilité complète des activités effectuées.

En regardant les différents fichiers de log, je me suis aperçu qu'il y avait certaines erreurs, j'ai donc commencé par paramétrer le multipathing sur notre système. Le multipathing permet d'améliorer la résilience et les performances du stockage en utilisant plusieurs chemins vers les périphériques de stockage. J'ai configuré les paramètres par défaut, ajouté des règles de liste noire et configuré un bloc spécifique pour les périphériques VMware. Cette configuration améliorera la résilience et les performances de notre stockage en utilisant plusieurs chemins vers les périphériques de stockage.

Ensuite, en milieu de semaine, j'ai entrepris la mise en place de l'extension LDAP dans Guacamole. Malgré quelques problèmes rencontrés lors de la configuration initiale, j'ai pu me connecter avec les utilisateurs de l'Active Directory. Cependant, je continue de travailler sur des paramètres permettant la création automatique des comptes utilisateurs dans la base de données Guacamole.

En fin de semaine, j'ai poursuivi mes efforts pour résoudre les problèmes liés à la création automatique des comptes utilisateurs dans Guacamole. Bien que je puisse me connecter avec les utilisateurs de l'Active Directory, les comptes utilisateurs ne sont toujours pas créés automatiquement dans la base de données, ce qui empêche l'accès aux machines virtuelles. Je cherche des solutions appropriées pour résoudre ce problème.

Puis, j'ai fait un peu de documentation notamment pour l'installation de l'extension Guacamole History Recording Storage sur la VM hébergeant Guacamole Apache. J'ai suivi un tutoriel et suivi les étapes d'installation recommandées. Cette extension permettra d'enregistrer les sessions vidéo et d'améliorer la traçabilité des activités.

Malgré quelques problèmes rencontrés tout au long de la semaine, j'ai pu mettre en place des mesures de sécurité, améliorer la gestion des chemins multiples et intégrer l'authentification LDAP dans Guacamole. Je suis toujours en train de résoudre le problème de création automatique des comptes utilisateurs. Je reste déterminé à trouver une solution pour garantir une expérience fluide et sécurisée à nos utilisateurs.